



Universidade de Brasília

Instituto de Ciências Exatas  
Departamento de Ciência da Computação

## **Desenvolvimento do módulo de Reconhecimento Facial para a Ferramenta em Análise Forense FI<sup>2</sup>**

Gustavo Carneiro Bicalho

Monografia apresentada como requisito parcial  
para conclusão do Bacharelado em Ciência da Computação

Orientador  
Prof. Dr. Flávio de Barros Vidal

Brasília  
2013

Universidade de Brasília — UnB  
Instituto de Ciências Exatas  
Departamento de Ciência da Computação  
Bacharelado em Ciência da Computação

Coordenadora: Prof.<sup>a</sup> Dr.<sup>a</sup> Maristela Terto de Holanda

Banca examinadora composta por:

Prof. Dr. Flávio de Barros Vidal (Orientador) — CIC/UnB

Prof. Dr. Díbio Leandro Borges — CIC/UnB

Jorge de Albuquerque Lambert — SEPAEL/DPF

### **CIP — Catalogação Internacional na Publicação**

Bicalho, Gustavo Carneiro.

Desenvolvimento do módulo de Reconhecimento Facial para a Ferramenta em Análise Forense FI<sup>2</sup> / Gustavo Carneiro Bicalho. Brasília : UnB, 2013.

97 p. : il. ; 29,5 cm.

Monografia (Graduação) — Universidade de Brasília, Brasília, 2013.

1. Ferramenta de Investigação de Imagens , 2. Reconhecimento Facial,  
3. Processamento de Imagens

CDU 004.4

Endereço: Universidade de Brasília  
Campus Universitário Darcy Ribeiro — Asa Norte  
CEP 70910-900  
Brasília-DF — Brasil



# Desenvolvimento do módulo de Reconhecimento Facial para a Ferramenta em Análise Forense FI<sup>2</sup>

Monografia apresentada como requisito parcial  
para conclusão do Bacharelado em Ciência da Computação

Prof. Dr. Díbio Leandro Borges    Jorge de Albuquerque Lambert  
CIC/UnB    SEPAEL/DPF

Prof.<sup>a</sup> Dr.<sup>a</sup> Maristela Terto de Holanda  
Coordenadora do Bacharelado em Ciência da Computação

Brasília, 6 de Março de 2013

# Resumo

A cada dia a investigação forense baseada em imagens e vídeos ganha mais importância, e com isso em mente, foi adicionado ao FI<sup>2</sup> suporte à vídeo e um módulo para reconhecimento facial. Para o desenvolvimento desse módulo, foi proposto um novo método para o reconhecimento facial, utilizando-se da região dos olhos para se obter uma métrica e poder realizar a comparação entre as faces.

**Palavras-chave:** Ferramenta de Investigação de Imagens , Reconhecimento Facial, Processamento de Imagens

# Abstract

Everyday the forensic investigation based on images and videos grows more important, and with that in mind, it was added to the FI<sup>2</sup> video support and a facial recognition module. To develop that module, it was proposed a new method for facial recognition, using the eye region to obtain a metric and be able to realize a comparison between faces.

**Keywords:** Image Investigation Tool, Facial Recognition, Image Processing

# Sumário

<b>1</b>	<b>Introdução</b>	<b>1</b>
<b>2</b>	<b>Reconhecimento Facial</b>	<b>3</b>
2.1	Introdução . . . . .	3
2.2	Desafios do reconhecimento facial forense . . . . .	5
2.2.1	Envelhecimento Facial . . . . .	5
2.2.2	Marcas Características na Face . . . . .	7
2.2.3	Reconhecimento com Retrato Falado . . . . .	8
2.2.4	Reconhecimento Facial em Vídeo . . . . .	9
<b>3</b>	<b>Ferramentas para análise forense de imagens digitais</b>	<b>11</b>
3.1	dTective . . . . .	11
3.2	Impress . . . . .	11
3.3	StarWitness . . . . .	12
3.4	A ferramenta FI <sup>2</sup> . . . . .	12
3.4.1	Arquitetura do programa . . . . .	12
3.4.2	Módulos . . . . .	14
3.4.3	Diagrama de Classes e Procedimento para inserção de novas ferramentas . . . . .	15
3.4.4	Registro de atividades - Log . . . . .	16
3.4.5	Ferramentas disponíveis . . . . .	17
3.5	Suporte a vídeo . . . . .	18
<b>4</b>	<b>Desenvolvimento do Módulo de Reconhecimento Facial</b>	<b>21</b>
4.1	Classe Cascade Classifier . . . . .	21
4.2	Exemplos da utilização de máscaras . . . . .	22
4.3	Detecção de faces na ferramenta FI <sup>2</sup> . . . . .	25
<b>5</b>	<b>Proposta de Método para Reconhecimento Facial</b>	<b>26</b>
5.1	Obtenção das medidas dos olhos . . . . .	26

5.2	Extração da métrica . . . . .	27
5.3	Comparação de faces . . . . .	28
<b>6</b>	<b>Resultados Obtidos</b>	<b>29</b>
6.1	Detecção facial e extração . . . . .	29
6.2	Reconhecimento facial . . . . .	31
6.2.1	Imagem de comparação 2 . . . . .	34
6.3	Avaliação da Métrica Proposta . . . . .	36
<b>7</b>	<b>Conclusão</b>	<b>38</b>
	<b>Referências</b>	<b>39</b>

# Lista de Figuras

2.1	Diferentes formas de como as fotos dos rostos estão quando obtidas para reconhecimento facial forense.[4]	4
2.2	Descrição do processo para reconhecimento facial forense[4]	5
2.3	Exemplos dos método discriminativo e generativo[4]	6
2.4	Processo de detecção automático de marcas[4]	7
2.5	Exemplo onde o testemunho gerou um desenho que acarretou em um reconhecimento falho[4]	9
2.6	Na primeira imagem temos um frame obtido pela câmera estática, enquanto no segundo temos a imagem de maior qualidade obtida pela câmera PTZ[4]	10
3.1	Diagrama de classes simplificado da ferramenta, já com a inserção do suporte a vídeo.	15
3.2	Diagrama mostrando como se inserir uma nova ferramenta.	16
3.3	Imagem para exemplificar o log.	17
3.4	Exemplo da ferramenta de correção de perspectiva.	18
3.5	Na parte inferior da imagem é possível observar a trackbar.	19
3.6	Exemplo do frame extraído.	20
4.1	Detecção de faces utilizando a máscara para faces frontais	22
4.2	Detecção de faces utilizando a máscara para olhos. Cada círculo azul é um objeto diferente	23
4.3	Detecção de faces utilizando a máscara para faces de perfil	23
4.4	Detecção de faces utilizando a máscara para nariz	24
4.5	Detecção de faces utilizando a máscara para bocas.	24
5.1	Fluxograma das etapas do método proposto.	26
6.1	Exemplo das configurações que podem ser escolhidas na ferramenta de identificação facial.	30
6.2	Exemplo da ferramenta em funcionamento, utilizando a máscara para rostos frontais. O rosto encontrado é extraído em uma nova janela.	30



6.3	Exemplo da ferramenta em funcionamento, utilizando a máscara para narizes. Com esse exemplo é possível observar a ocorrência de falsos positivos, isto é, objetos que não são narizes sendo detectados. . . . .	31
6.4	Exemplo de face utilizada para comparação. . . . .	32
6.5	Exemplo do reconhecimento, utilizando a imagem 6.4. Apesar de na imagem de comparação os olhos estarem com formas diferentes, ainda foi possível realizar o reconhecimento devido à margem de erro. . . . .	32
6.6	Utilizando a mesma imagem de comparação, nenhuma face foi detectada. Ao encontrar uma face compatível, ela é recortada para a <i>SubWindow</i> ao lado. O motivo de não ter detectado, é a abertura dos olhos. . . . .	33
6.7	Exemplo de face utilizada para comparação. . . . .	34
6.8	Exemplo onde mesmo com o rosto não estando completamente voltado para câmera, foi possível realizar o reconhecimento. . . . .	34
6.9	Exemplo com margem de erro de 20% utilizando a imagem de comparação acima, onde o rosto encontrado não é o mesmo indivíduo da imagem. . . .	35
6.10	Diminuindo a margem de erro para 10%, o indivíduo não é mais reconhecido como sendo o mesmo sujeito da imagem de comparação. . . . .	36

# Lista de Tabelas

3.1	Tabela com os módulos presentes na ferramenta antes do início desse projeto.	14
3.2	Tabela mostrando os módulos e as funcionalidades que podem ser inseridas.	14
6.1	Tabela com os resultados obtidos no teste. VP = verdadeiro positivo, VN = verdadeiro negativo, FP = falso positivo, FN = falso negativo. . . . .	37

# Capítulo 1

## Introdução

O processo de investigação forense utiliza um conjunto de recursos para que o objetivo seja alcançado, com isso o uso de fotos e vídeos se torna bastante relevante. Porém a utilização desses recursos pode esbarrar em algumas barreiras, como vídeos de baixa qualidade ou ângulos que não proporcionam uma boa visualização. A tecnologia atual permite que essas barreiras possam ser transpostas e resultados satisfatórios para a investigação forense possam ser obtidos.

O reconhecimento facial automático, por ser uma área recente de pesquisa, ainda é pouco explorado na prática de investigações forenses uma vez que é necessário um grande poder de processamento de imagens, a identificação de uma face dentro de um banco de dados é um processo que demanda um elevado custo computacional. Mas, com o desenvolvimento de novas técnicas e algoritmos, a realidade está mudando, e esta área de pesquisa está se tornando cada vez mais relevante para processos de investigação forense. Esse crescimento faz com que sejam desenvolvidos sistemas capazes de auxiliar a investigação policial no reconhecimento de indivíduos.

A Ferramenta de Investigação de Imagens(FI<sup>2</sup>)[3] foi desenvolvida com o intuito de ajudar as investigações que utilizam imagens. Esta ferramenta permite realizar operações na imagem com o propósito de facilitar o trabalho dos investigadores forenses e permitir que sejam obtidas informações antes impossíveis devido ao mal estado das imagens. Algumas das funcionalidades já implementadas na ferramenta são: cortar imagem, alteração da luminância e do contraste, girar/rotacionar a imagem. Além disso, por se tratar de uma ferramenta voltada para fins forenses, existe um registro de atividades(log) onde as operações realizadas sobre a imagem são registradas, certificadas, e explicações sobre os algoritmos utilizados para que possa ser reproduzido por outra pessoa.

Os objetivos deste trabalho são: o estudo das técnicas e algoritmos de reconhecimento facial [1] [2], adicionar suporte à vídeo na Ferramenta de Investigação de Imagens(FI<sup>2</sup>)[3] e a criação de um módulo para a realização do reconhecimento facial onde o suspeito é

colaborador ou em condições favoráveis. Para que os objetivos sejam alcançados serão utilizadas bibliotecas e ferramentas já existentes, como o openCV [5] [8] e o QT [7].

O capítulo 2 apresenta uma introdução sobre o reconhecimento facial e seus desafios. O capítulo 3 são apresentadas ferramentas para análise forense de imagens digitais e as principais características da ferramenta FI<sup>2</sup>. O capítulo 4 trata do módulo de reconhecimento facial dentro da ferramenta. O capítulo 5 apresenta uma proposta de método para reconhecimento facial. No capítulo 6 temos os resultados obtidos. E finalmente no capítulo 7 temos as conclusões deste projeto.

# Capítulo 2

## Reconhecimento Facial

### 2.1 Introdução

Reconhecimento facial é a capacidade de identificar um indivíduo baseado nas características biométricas de sua face. Automatizar esse processo vem sendo alvo de estudos nas últimas décadas devido a sua vasta área de aplicação, por exemplo: segurança das vias e verificação de documentos de identidade. Um sistema de reconhecimento de imagem normalmente trabalha sobre dois cenários, verificação e identificação. No primeiro, a similaridade entre duas imagens contendo as faces são medidas e é determinado se há compatibilidade. No segundo cenário, a imagem da face é comparada com um vasto número de imagens armazenadas em um banco de dados e se obtém como retorno o indivíduo que mais se assemelha a partir de uma métrica definida, e dessa forma se tem uma possível identificação do indivíduo. A ideia é que, em ambos os cenários, seja possível realizar a identificação automática.

A performance de técnicas para reconhecimento automatizado são avaliadas em vários testes realizados pelo National Institute of Standards and Technology(NIST) utilizando o método de avaliação FERET [9]. No teste FRVT 2002(Face Recognition Vendor Test), foi obtida uma acurácia de 70% para imagens frontais e condições normais de luz(foram utilizadas 121.589 imagens de 37.437 indivíduos). O teste mais recente foi o FRVT 2006, onde o melhor sistema mostrou uma excelente performance, dando uma taxa de falso negativo de 0.01 e uma taxa de falso positivo de 0.001.

Apesar desses resultados para sistemas de reconhecimentos faciais automatizados, eles não refletem a acurácia de sistemas quando utilizados em ambientes em que não é possível controlar a luminosidade e a posição do indivíduo. As tentativas de utilização de sistemas de reconhecimento facial automatizados em situações reais não obtiveram níveis suficientes de acurácia [4]. Porém, algumas aplicações já vem sendo utilizadas com sucesso, como é o caso do Smartgate na Austrália [10], neste caso o usuário coopera para que o ambiente seja

favorável para o reconhecimento. Além dessas variáveis, um sistema forense deve lidar com variações intrínsecas como envelhecimento, maquiagem e expressão facial. Esses fatores também diminuem a performance das técnicas e normalmente não são levados em consideração nos estudos.



Figura 2.1: Diferentes formas de como as fotos dos rostos estão quando obtidas para reconhecimento facial forense.[4]

Ao contrário de testes como de DNA e da impressão digital, que possuem um grau de significância grande dentre os métodos da ciência forense, o reconhecimento facial automatizado deve passar por uma melhoria em suas ferramentas para se determinar a identidade de uma pessoa. Esse progresso é um dos objetivos de vários órgãos interessados no assunto, incluindo o FBI[4].

De acordo com o artigo [4] o reconhecimento facial forense se separa um pouco do automatizado, pois requer a participação de um humano no processo. Existem alguns fatores para que isso seja necessário, como: má qualidade da imagem para comparação, necessidade de mostrar a evidência nos tribunais e a utilização de características particulares das faces para aumentar a acurácia[4]. Um processo típico de reconhecimento facial forense inicia com uma grande quantidade de imagens, como fotos de identificação criminal ou de documentos de identidade. Em seguida, é utilizado um sistema de reconhecimento facial automatizado para poder fazer comparações em um banco de dados grande. Como a imagem de comparação nem sempre está nas condições ideais para comparação, as com maiores graus de similaridade são selecionadas, gerando um conjunto muito reduzido de imagens. Com esse número reduzido de possíveis suspeitos, um perito irá analisar para determinar o suspeito correto. A figura 2.2 mostra uma representação do processo de reconhecimento facial.

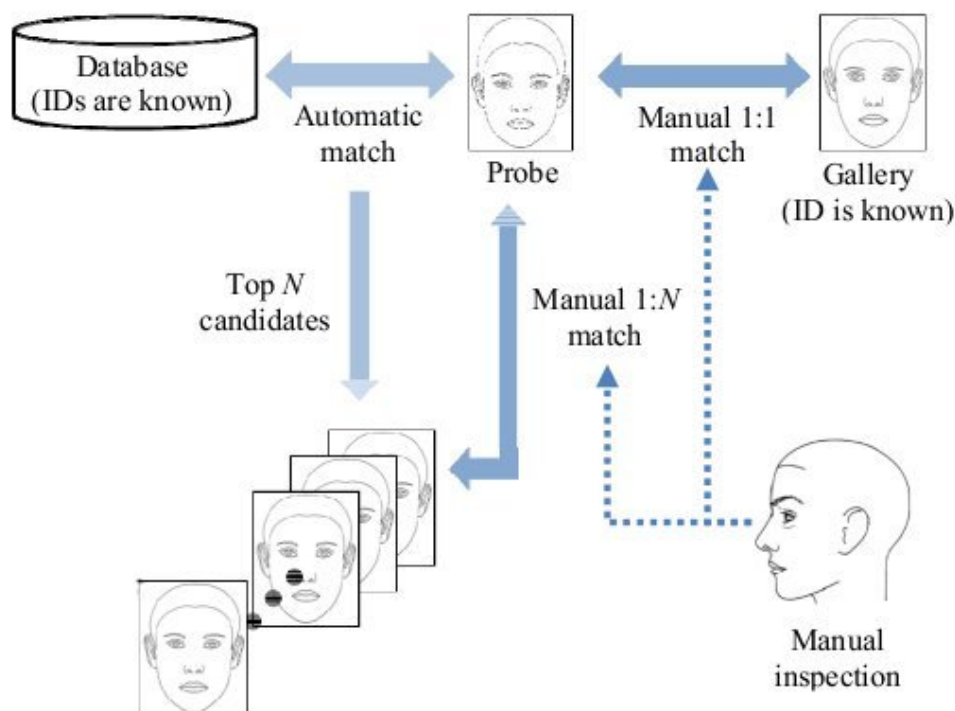


Figura 2.2: Descrição do processo para reconhecimento facial forense[4]

## 2.2 Desafios do reconhecimento facial forense

O reconhecimento facial tem esbarrado em diversos desafios, como: envelhecimento da face, problemas com luminosidade da imagem e má qualidade das câmeras de vigilância. Porém, a tecnologia tem evoluído para diminuir os efeitos dessas adversidades, e melhorar a capacidade de realizar um reconhecimento facial.

### 2.2.1 Envelhecimento Facial

Muitas das vezes, a imagem do indivíduo que se tem guardada no banco de dados tem anos de diferença com a imagem utilizada para comparação. Quanto maior a diferença de idade entre as imagens, a chance de se obter um reconhecimento entre as imagens diminui. Essa situação pode ocorrer em casos como identificação de uma criança desaparecida ou procurar se um suspeito está presente no banco de dados da polícia.

O processo de envelhecimento facial é complexo e afeta diretamente o formato e a textura do rosto. Esse processo pode variar de acordo com a idade, por exemplo em grupos de pessoas mais jovens(até 18 anos) em que caracteriza pelo crescimento do rosto. Já para grupos de pessoas mais velhas(acima de 18 anos), o processo é caracterizado mais pela mudança da textura do que por mudanças no formato do rosto. Além do envelhecimento da face, outros fatores podem influenciar na aparência do rosto como a luz, expressão e pose, o que pode dificultar o estudo do padrão de envelhecimento.

Existem dois modelos de envelhecimento para reconhecimento facial, definidos como o generativo e o discriminativo. O modelo generativo utiliza um modelo de envelhecimento paramétrico em um domínio 3D para gerar imagens sintéticas e diminuir a diferença de idade entre a imagem de prova e as imagens que se tem no banco de dados. Esse modelo também utiliza métodos para correção da pose. O modelo discriminativo utiliza de características do rosto para conseguir reconhecer não importando a diferença de idade entre ambas as imagens. Em teste[4] realizado com 10.000 imagens e 10.000 indivíduos, foi notado um aumento significativo na identificação exata com a utilização desses dois modelos de envelhecimento.

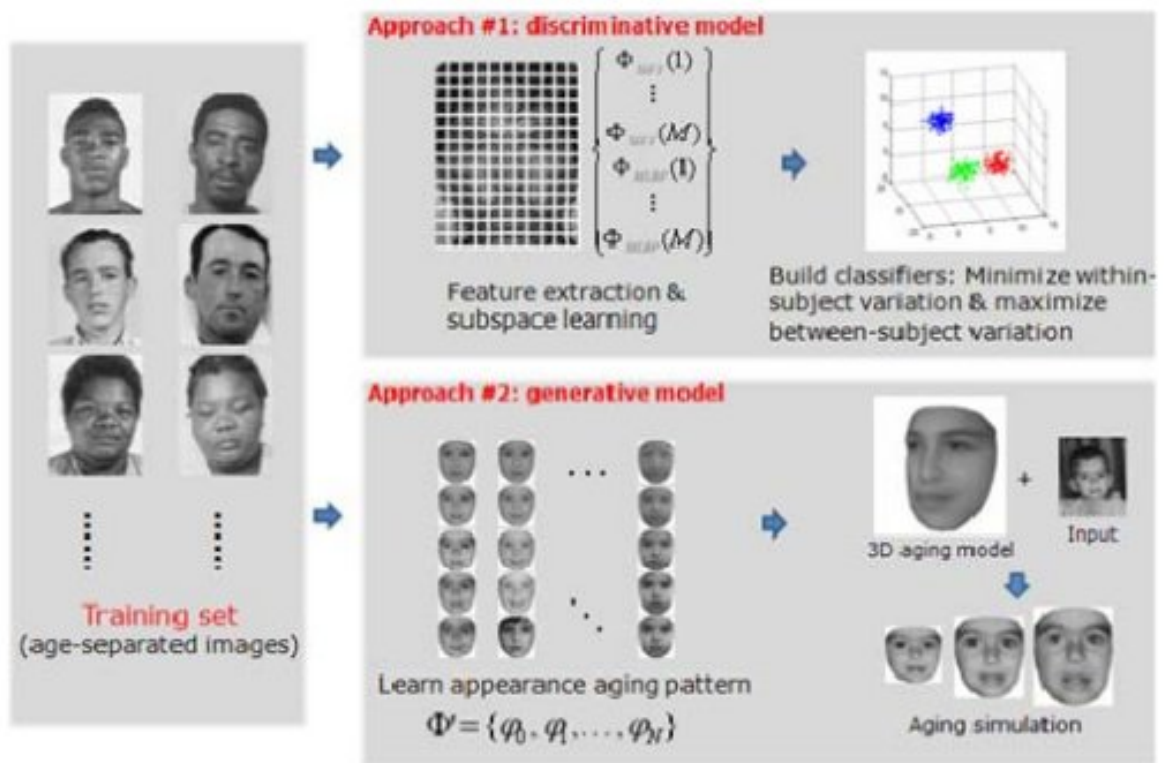


Figura 2.3: Exemplos dos método discriminativo e generativo[4]



## 2.2.2 Marcas Características na Face

Características na face como cicatrizes, verrugas e sardas tem um papel muito importante para a identificação de rostos em aplicações forenses. A utilização dessas características se tornou importante devido às facilidades de serem percebidas com sensores de maior qualidade, compatibilidade com identificação manual e o crescente aumento dos bancos de dados de imagens faciais. A partir dessas marcas na face é possível aumentar tanto a acurácia como a velocidade da identificação dos sistemas de reconhecimento facial. Essas informações também são importantes para o testemunho dos peritos, onde é esperado que cheguem a uma conclusão em relação a identidade dos suspeitos.

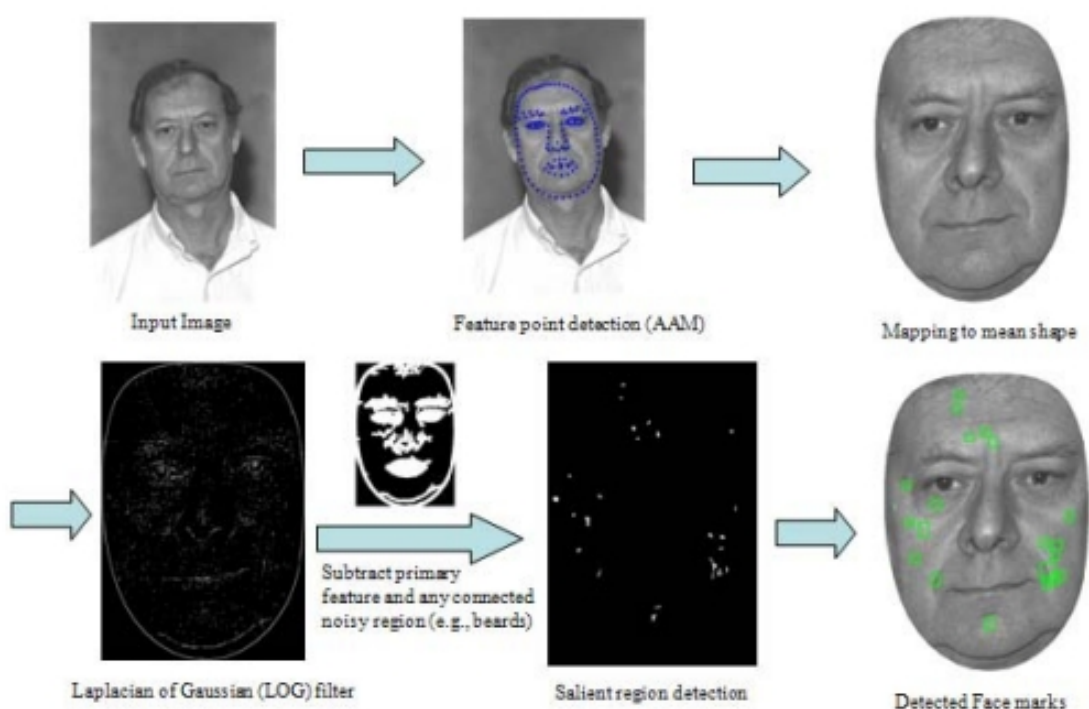


Figura 2.4: Processo de detecção automático de marcas[4]

A maioria das identificações por foto envolve um estágio de identificação manual. A informação da identificação normalmente é fornecida pela vítima por meio de uma descrição verbal ou retratos falados. O processo de exame facial utilizado atualmente em investigações legais tem como principal fase identificar a classe (formato do rosto, cor do cabelo, pelos faciais, formato do nariz, sardas, etc) e as características individuais (número e localização de pintas, cicatrizes, tatuagens, etc) no rosto do indivíduo. Automatizar o processo de localizar essas características não apenas irá reduzir a subjetividade do trabalho manual, mas também tornará o processo mais consistente e preciso. Além disso,

irá padrozinhar todo o processo de examinação dessas características e o tornará mais eficiente.

Padrões de marcas na face tem se mostrado confiáveis para algumas das características biométricas. Existem sistemas[4] capazes de, a partir de uma entrada textual, obter uma lista de suspeitos que contém a característica requerida como por exemplo: "Cicatriz na bochecha direita".

O objetivo desses sistemas não é obter um único suspeito, e sim diminuir a quantidade de candidatos em que se deverá realizar a busca. Em uma situação em que não há nenhuma imagem para comparação com as do banco de dados, esses sistemas ainda poderão ser utilizados para se obter uma lista reduzida dos suspeitos. Juntando as marcações facias com altura, idade e sexo, o investigador terá em suas mãos um grupo menor de suspeitos para analisar.

Além de permitir obter uma comparação sem ter uma imagem do rosto por completo, marcações no rosto se mostram cruciais para identificação de gêmeos idênticos. Com a utilização desses métodos, foi possível observar um aumento de 0.5% de acerto na identificação em testes realizados com 213 imagens para comparação de 213 indivíduos distintos em um banco de dados com 10.213 imagens de 10.213 indivíduos.

### 2.2.3 Reconhecimento com Retrato Falado

Frequentemente não se tem nenhuma foto do suspeito disponível. Quando isso ocorre, pode-se utilizar um retrato falado do suspeito. Ou seja, a representação artística da aparência do rosto de uma pessoa a partir das descrições de uma testemunha ocular. Essa representação nem sempre será correta e pode conter erros devidos à memória da testemunha ou algum outro fator, como ansiedade e transtorno pós-traumático.

Os sistemas de reconhecimento facial comerciais não são desenvolvidos para comparar um retrato falado com uma fotografia real do rosto de uma pessoa. Para preencher essa lacuna, foi desenvolvido um *framework* para realizar essa comparação. A idéia é utilizar dicas marcantes para descrever tanto a imagem como o desenho, e assim é feita a comparação em ambos. Uma melhora significativa foi observada para os testes realizados e atualmente a *framework* Local Feature-based Discriminant Analysis(LFDA) é necessária para se maximizar a capacidade forense de reconhecimento a partir de retratos falados.

Uma grande dificuldade nessa área é a incapacidade da testemunha de relatar corretamente a aparência do suspeito. Esse problema também se estende para o reconhecimento automático por retratos falados, fazendo com que ocorra erros na identificação e podendo fazer que leve pessoas inocentes a serem considerados os principais suspeitos.



Figura 2.5: Exemplo onde o testemunho gerou um desenho que acarretou em um reconhecimento falho[4]

#### 2.2.4 Reconhecimento Facial em Vídeo

O reconhecimento facial em vídeo vem ganhando importância devido ao grande crescimento do número de câmeras de segurança espalhadas pelas cidades. A capacidade de automaticamente reconhecer faces em um vídeo em tempo-real irá facilitar os métodos de identificação podendo fazer uso das redes de câmeras de segurança existentes. Uma dificuldade encontrada nesse tipo de reconhecimento é que normalmente as imagens obtidas das faces nem sempre são frontais e podem estar sujeitas a mudanças de iluminação. A captura de vários frames do mesmo indivíduo em uma vídeo permite que o sistema possa selecionar a imagem do rosto com a melhor qualidade: frontal, na expressão natural e luminosidade correta. É possível utilizar informações temporárias como a mudança de expressões faciais, no reconhecimento. Como as câmeras comuns de segurança utilizam baixa qualidade, é possível com o uso de uma câmera estática e uma câmera PTZ(câmera capaz de direcionamento remoto e controle de zoom) melhorar o resultado na identificação. A câmera estática informa a câmera PTZ a presença de um indivíduo, e assim a câmera PTZ obtêm uma imagem de maior qualidade da imagem da pessoa.

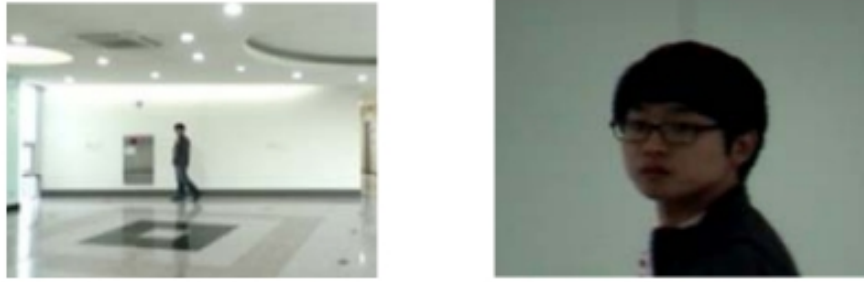


Figura 2.6: Na primeira imagem temos um frame obtido pela câmera estática, enquanto no segundo temos a imagem de maior qualidade obtida pela câmera PTZ[4]

Existem métodos para resolver o problema da posição do rosto e da variação de luz do indivíduo. Foi proposto um método para se obter uma imagem 3D de um rosto, a partir de uma imagem 2D, necessitando apenas de uma única imagem do rosto em uma pose arbitrária, porém o processo pode levar alguns minutos e requer um alinhamento inicial manual. A utilização dessa modelagem 3D e da câmera PTZ fez com que a acurácia aumentasse em números consideráveis.

# Capítulo 3

## Ferramentas para análise forense de imagens digitais

Atualmente existem várias ferramentas para a análise forense. Nesse capítulo serão mostradas algumas ferramentas para análise de imagens e vídeos. Primeiramente serão mostradas as funcionalidades de cada ferramenta e em seguida um comparativo com a ferramenta FI<sup>2</sup>, além de mostrar suas principais características, e aplicações. As principais ferramentas utilizadas para fins forenses são: dTective, Impress, Star Witness.

### 3.1 dTective

Desenvolvido pela Ocean Systems[13], dTective é o sistema utilizado pelo *Federal Bureau of Investigation*(FBI) e pela *Central Intelligence Agency*(CIA), além de outras organização em todo o mundo.

O dTective tem como características poder trabalhar com imagem digital ou analógica, capacidade de melhorar a qualidade e a luminosidade de vídeos, possibilidade de inserir comentários relacionados ao vídeo e ferramentas para melhoria de imagens. Porém é um código fechado e não foi encontrado nenhuma informação sobre armazenamento de log.

### 3.2 Impress

Desenvolvido pela IMIX[12]. O Impress tem como características utilizar algoritmos de processamento de imagem para restaurar, melhorar e extrair informações, além disso possui interface simples e pode armazenar o log, porém tem como desvantagem ser um código fechado.

### 3.3 StarWitness

Desenvolvido pela Signalscape[11]. Disponibiliza um sistema completo para análise forense de imagens, fornecendo tanto o hardware como o software necessário. O StarWitness tem como características trabalhar com qualquer formato digital de vídeo, permitir trabalhar com câmeras em tempo real, diversas ferramentas para se trabalhar com vídeo e permite a análise de áudio.

### 3.4 A ferramenta FI<sup>2</sup>

A ferramenta FI<sup>2</sup>[3], em comparação com as citadas acima, tem como principal características ser um código aberto, possibilitando que se saiba exatamente o que cada algoritmo utilizado faz com a imagem ou vídeo. Além disso, possui uma arquitetura que permite que novas funcionalidades sejam facilmente implementadas de acordo com as necessidades encontradas.

A Ferramenta proposta, atualmente, tem as seguintes principais características:

- É um software modular, ou seja, dividido em diversos módulos, cada um com a sua funcionalidade. Dessa forma, o incremento de uma nova funcionalidade se torna fácil.
- É toda desenvolvida em C++ e utiliza bibliotecas *opensource*, como o OpenCV, para o processamento de imagem, e o QT para interface com o usuário.
- A ferramenta tem portabilidade entre sistemas operacionais, podendo tanto ser usada em plataformas Windows, como Linux e MacOS.
- As funcionalidades desenvolvidas foram projetadas para uso em análise pericial.
- Todas as atividades realizadas são registradas em um log, possibilitando que essas operações sejam reproduzidas.
- Capacidade de se trabalhar com imagens e vídeos, ampliando o número de aplicações da ferramenta.

#### 3.4.1 Arquitetura do programa

O sistema foi projetado para ter três principais objetivos:

- Desempenho
- Portabilidade
- Escalabilidade

## **Desempenho**

Como algumas das técnicas de processamento de imagens demandam um elevado poder de processamento, o desempenho se torna um fator essencial para a ferramenta. Associado a isso, deseja-se resposta rápida, com o intuito de o operador obter um resultado o mais célere possível para cada alteração de parâmetro de uma determinada operação, facilitando, assim, a comparação entre as diversas configurações possíveis de uma determinada técnica. Para satisfazer esse requisito, decidiu-se pelo projeto de uma aplicação nativa, utilizando-se a linguagem C++, que é servida de compiladores nas mais diversas plataformas.

## **Portabilidade**

A portabilidade é um aspecto importante tendo em vista o reaproveitamento de códigos e a alcançabilidade da ferramenta. Para obter a almejada portabilidade, estudou-se, dentre as possibilidades, ferramentas que pudessem ser interoperadas indistintamente entre os três principais sistemas operacionais: Windows, MacOS e Linux. Com isso, optou-se pelas bibliotecas OpenCV[8], para o auxílio no processamento de imagens, e QT[7] para o desenvolvimento da interface.

## **Escalabilidade**

A escalabilidade é importante pelo fato de se desejar uma ferramenta que englobe as mais diferentes e recentes ferramentas voltadas à investigação forense. Tais ferramentas têm os mais diversos requerimentos, tanto a interface quanto as características internas do programa. Para isso, desenvolveu-se uma interface única para o código de representação gráfica de todas as ferramentas e outra interface, também única, para encapsular o código de processamento de imagens das ferramentas, flexíveis o suficiente para atenderem as demandas que as ferramentas que se deseje implementar requerem.

### 3.4.2 Módulos

Módulos	Tarefas	Observações
Módulo 1	Ferramentas Básicas	Cortar Luminância e Contraste Conversão em escala cinza Girar/Rotacionar
Módulo 2	Interpolação	Vizinho mais próximo Bilinear Bicúbica Lanczos
Módulo 3	Operação de Pontos	Equalização de histograma
Módulo 4	Restauração de imagem	Correção de perspectiva

Tabela 3.1: Tabela com os módulos presentes na ferramenta antes do início desse projeto.

Módulos	Tarefas	Observações
Módulo 1	Ferramentas Básicas	
Módulo 2	Interpolação	
Módulo 3	Operação de Pontos	Binzarização Binarização adaptativa Alongamento de Contraste Operação logaritmica Operação Exponencial
Módulo 4	Filtros	Mediana Unsharp máscara(USM) Passa-altas Rational sharpening Média Passa-baixas Suavização de ruído Redução de artefatos de bloqueio Adicionar ruídos (teste) Laplace da Gaussiana Frequência

Tabela 3.2: Tabela mostrando os módulos e as funcionalidades que podem ser inseridas.



### 3.4.3 Diagrama de Classes e Procedimento para inserção de novas ferramentas

Inserir uma nova ferramenta no sistema é um processo relativamente fácil. Dessa forma, é possível que as necessidades individuais de cada usuário sejam cumpridas e permite um crescimento colaborativo da ferramenta, sem que seja necessário grandes modificações. As figuras 3.1 e 3.2 ilustram essa facilidade:

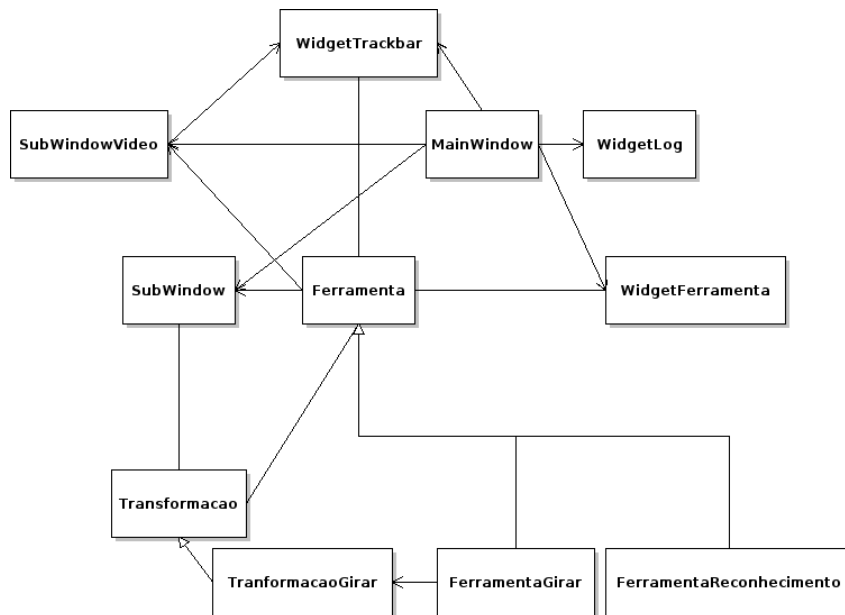


Figura 3.1: Diagrama de classes simplificado da ferramenta, já com a inserção do suporte a vídeo.

Na figura 3.1 é possível ver a estrutura das classes. Todas as classes de ferramentas herdam da classe **Ferramenta**. No caso dos vídeos, teremos a adição de um *Widget* para a *Trackbar* e de uma *SubWindow* destinada a vídeos.

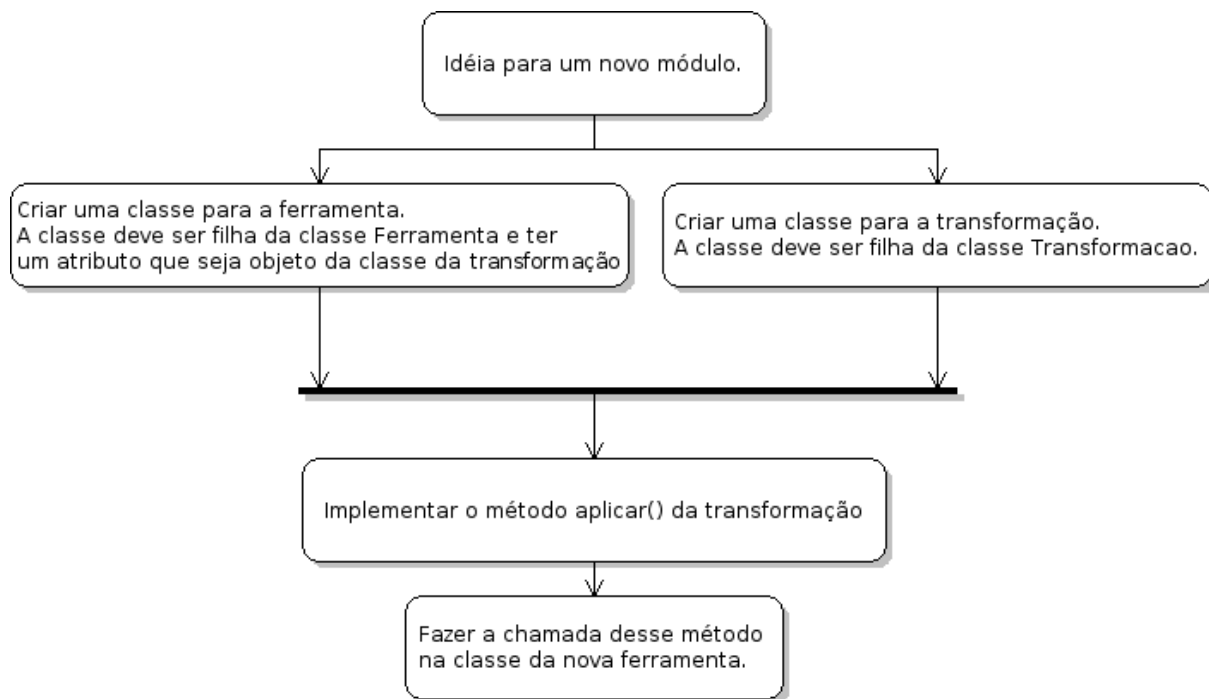


Figura 3.2: Diagrama mostrando como se inserir uma nova ferramenta.

Como é visto na figura 3.2, para se adicionar uma nova ferramenta, é necessário apenas uma classe para a nova ferramenta e uma para a transformação a ser realizada na imagem. A classe Ferramenta irá controlar os parâmetros que serão aplicados na transformação, e a classe Transformação, com o método aplicar(), irá realizar as operações na imagem e retornar a imagem processada.

#### 3.4.4 Registro de atividades - Log

Uma das principais características do sistema proposto é o log. Para que a perícia possa ser utilizada na produção de provas judiciais, é necessário que seja possível a sua reprodução. Com esse intuito, o sistema armazena todas as ações realizadas junto com o usuário que as realizou e a data e hora em que foi realizada determinada modificação nos arquivos originais.

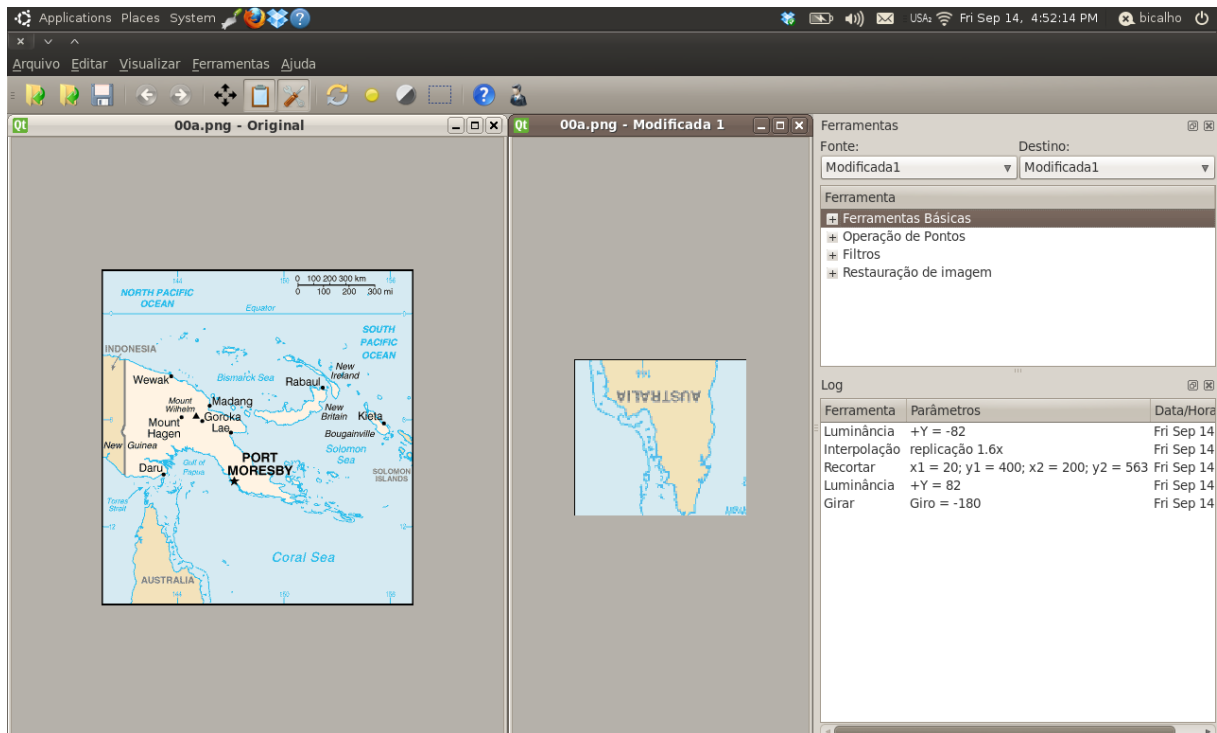


Figura 3.3: Imagem para exemplificar o log.

Na imagem 3.3, é possível ver o *Widget* de log registrando as atividades realizadas para se obter a nova imagem processada. Essa nova imagem pode ser salva, juntamente com o log das atividades. Caso seja necessário modificar a imagem novamente depois, o log das atividades será incrementado, possibilitando então que ao final da perícia seja possível obter todo o histórico das operações realizadas durante o exame.

### 3.4.5 Ferramentas disponíveis

A ferramenta FI<sup>2</sup> atualmente possui operações básicas de processamento de imagem, como: cortar, recortar, girar, interpolação e alterar contraste e luminância. Porém também contém outras mais complexas como a correção de perspectiva.

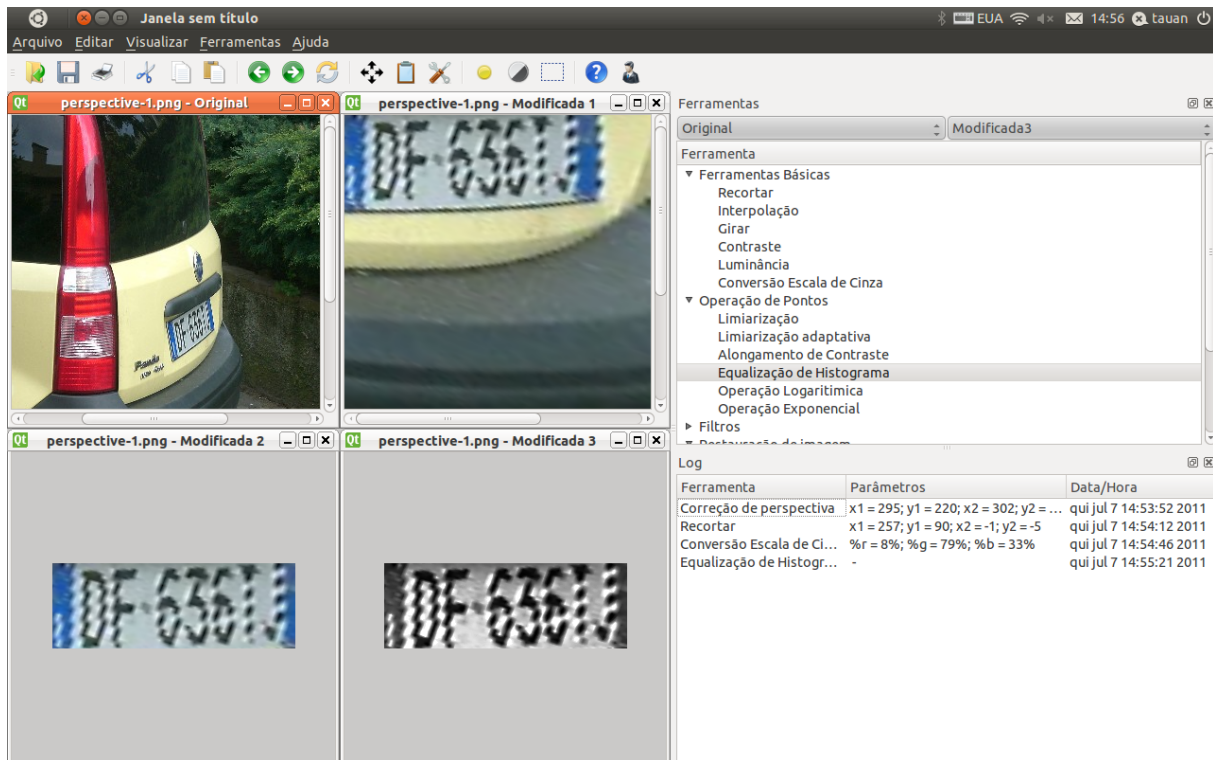


Figura 3.4: Exemplo da ferramenta de correção de perspectiva.

A imagem 3.4 mostra uma imagem onde não era possível identificar a placa do carro, porém com o auxílio de algumas funcionalidades do sistema, fica claro qual a placa do veículo da foto.

### 3.5 Suporte a vídeo

Para poder inserir suporte a vídeo, foi necessária a criação de uma *SubWindow* própria para isso e um *Widget* para a *trackbar*.

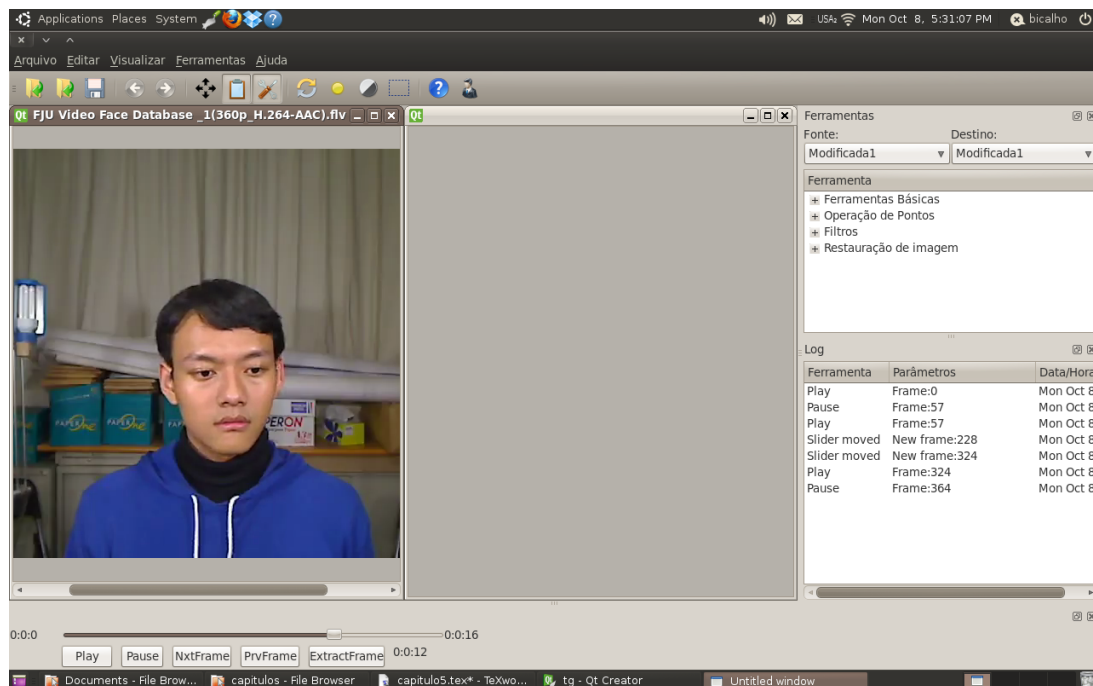


Figura 3.5: Na parte inferior da imagem é possível observar a trackbar.

Como visto na figura acima, o vídeo está sendo mostrado na *SubWindow* da esquerda, abaixo dessa janela é possível observar diversos botões:

- Play - Inicia a apresentação do vídeo do ponto em que parou.
- Pause - Para o vídeo.
- NxtFrame - Avança um frame no vídeo.
- PrvFrame - Volta um frame no vídeo.
- ExtractFrame - Extrai o frame atual para a subjanela da direita, é possível utilizar as diversas funcionalidades da ferramenta em cima do frame extraído.

Ainda é possível observar na imagem o log das ações que foram realizadas no vídeo para que seja possível a sua reprodução.

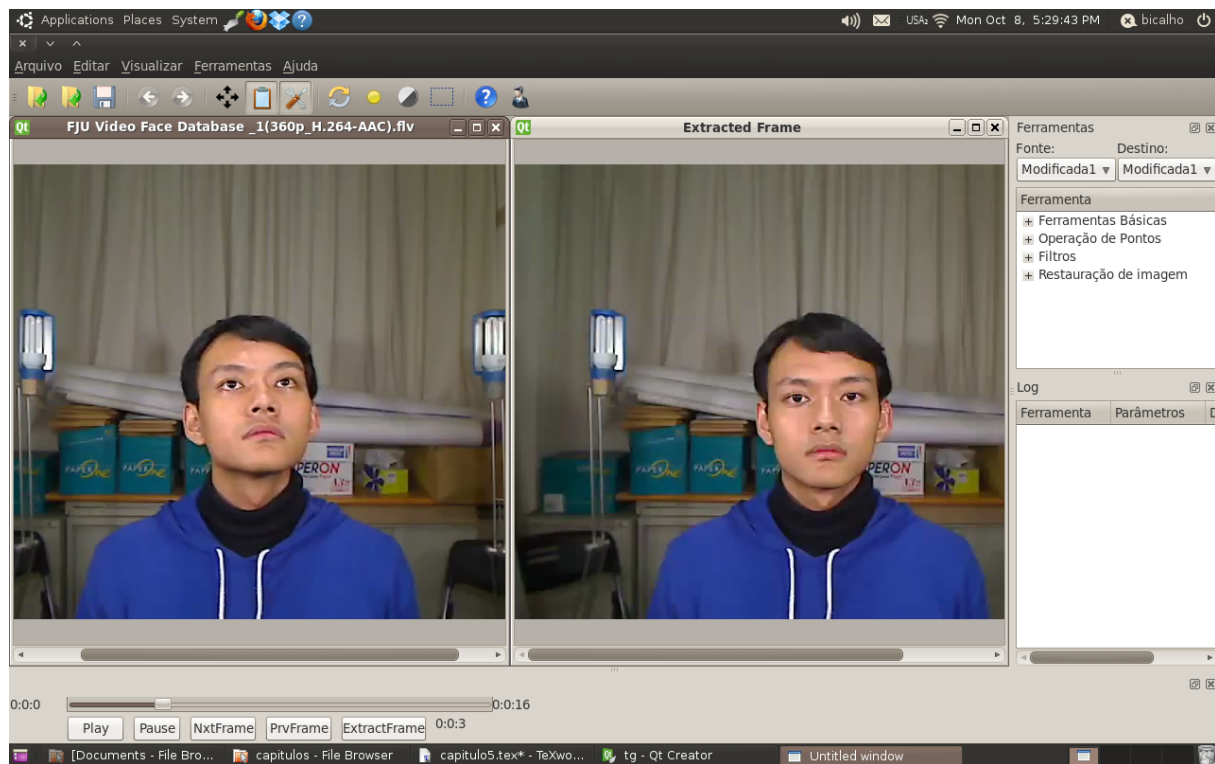


Figura 3.6: Exemplo do frame extraído.

# Capítulo 4

## Desenvolvimento do Módulo de Reconhecimento Facial

A ferramenta FI<sup>2</sup> é capaz de isolar as faces de um vídeo automaticamente facilitando assim a comparação com os possíveis suspeitos. Para que isso seja possível é utilizada uma classe do OpenCV que permite detectar um rosto ou qualquer outro objeto, desde que haja um treinamento, para isso.

### 4.1 Classe Cascade Classifier

A classe utilizada é a *CascadeClassifier*. Existem dois métodos que são essenciais para o funcionamento da ferramenta:

- `load(const string filename)`  
Carrega um classificador a partir de um arquivo.  
Parâmetros:
  - `filename` - Nome do arquivo com o treinamento para que seja possível identificar o objeto desejado.
- `detectMultiScale(const Mat image, vector<Rect> objects, double scaleFactor=1.1, int minNeighbors=3, int flags=0, Size minSize=Size(), Size maxSize=Size())`  
Detecta os objetos e retorna suas posições em uma lista de retângulos.  
Parâmetros:
  - `image` - Imagem onde deve ser detectado o objeto.
  - `objects` - Vetor de retângulos onde serão guardados os objetos detectados.
  - `scaleFactor` - Ajuste de escala da imagem

- minNeighbors - Mínimo de vizinhos que o objeto deve ter para que ele seja armazenado.
- flags - Não utilizado nas versões mais recentes de classificadores.
- minSize - Tamanho mínimo do objeto. Objetos menores serão descartados.
- maxSize - Tamanho máximo do objeto. Objetos maiores serão descartados.

## 4.2 Exemplos da utilização de máscaras

Existem diversas máscaras que podem ser utilizadas para a detecção de faces, dentre elas algumas possuem uma maior relevância para a área forense. Nessa sessão serão descritos exemplos do uso das seguintes máscaras

- Rosto frontal
- Olhos
- Rosto de perfil
- Nariz
- Boca



Figura 4.1: Detecção de faces utilizando a máscara para faces frontais





Figura 4.2: Detecção de faces utilizando a máscara para olhos. Cada círculo azul é um objeto diferente

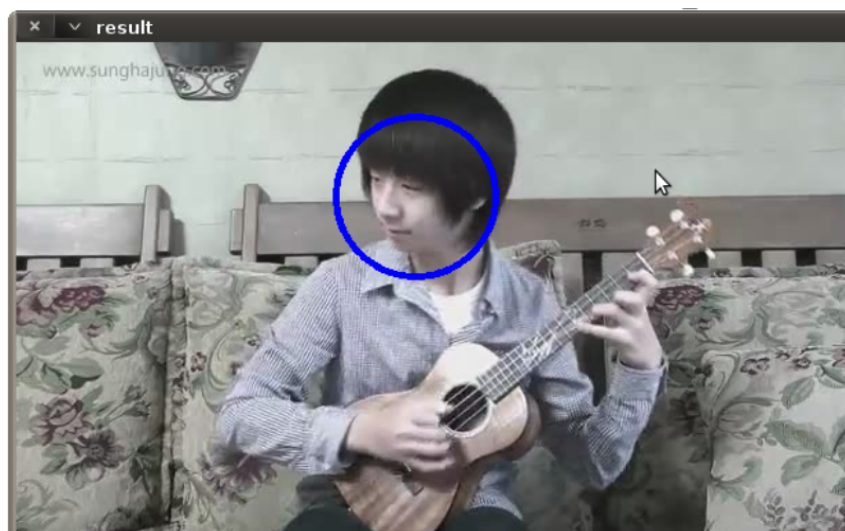


Figura 4.3: Detecção de faces utilizando a máscara para faces de perfil

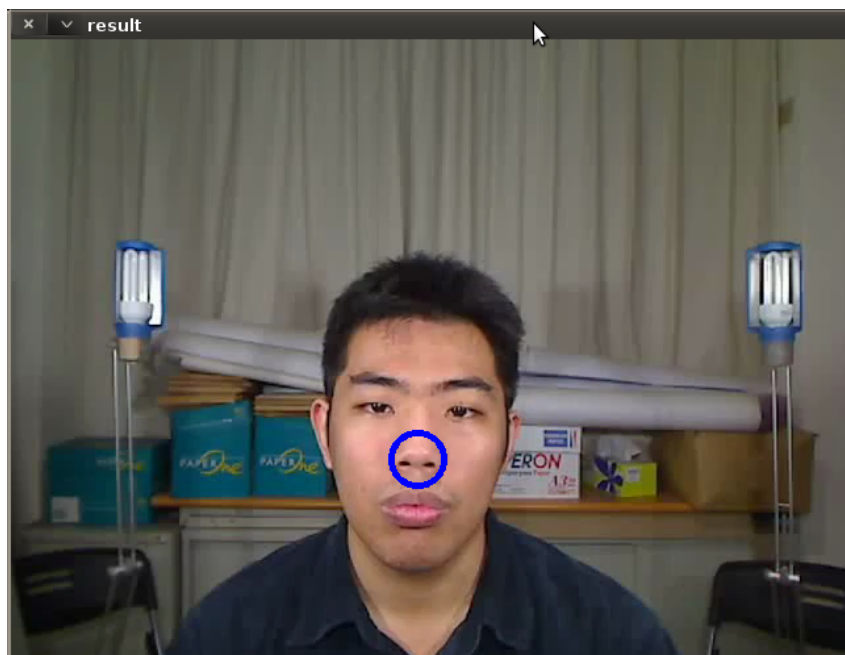


Figura 4.4: Detecção de faces utilizando a máscara para nariz

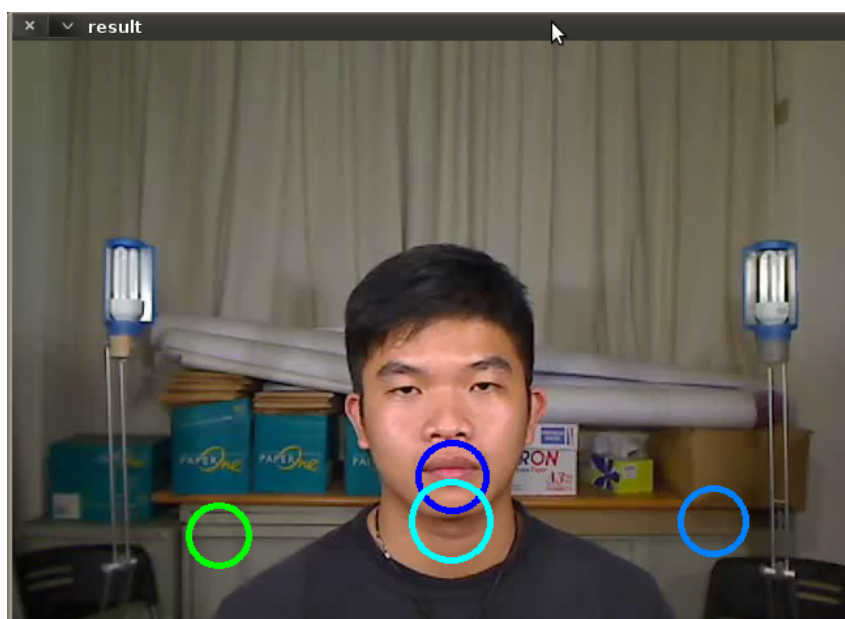


Figura 4.5: Detecção de faces utilizando a máscara para bocas.

No exemplo da figura 4.5 é possível presenciar a ocorrência de vários falsos positivos. Porém, como a intenção é utiliza-las em um sistema híbrido (parte automática, parte manual), esses falsos positivos podem ser facilmente descartados por um perito. Algumas

máscaras funcionam melhor que outras e com isso é necessário escolher a que melhor se adequa à necessidade da perícia.

Problemas maiores ocorrem quando acontecem falsos negativos, ou seja, os rostos não foram detectados. Com essa ocorrência será necessário que o perito manualmente extraia as faces do vídeo.

### 4.3 Detecção de faces na ferramenta FI<sup>2</sup>

No sistema proposto, esses rostos serão extraídos automaticamente para outra janela, excluindo o restante da imagem, com o intuito de facilitar o trabalho pericial. Além disso, todos os rostos distintos encontrados são armazenados em uma lista de faces, tornando possível que todos os rostos de um vídeo sejam comparados com uma imagem do rosto de um sujeito.

A distinção dos rostos é feita de maneira simples, utilizando uma redução de suavização espacial, de forma que se um rosto for visto em vários frames seguidamente, ele só será identificado como um novo rosto caso haja uma grande distância entre os pixels da posição central da face de um frame para outro.

## Capítulo 5

# Proposta de Método para Reconhecimento Facial

O desenvolvimento de um método para o reconhecimento facial é o foco principal desse trabalho, e apesar do OpenCV possuir funções para tal feito, estas precisam de um treinamento prévio ou uma base de dados com várias imagens do mesmo indivíduo para que funcionem. Foi proposto um novo método para se realizar o reconhecimento facial, baseado nas informações métricas da região dos olhos de uma pessoa. Os passos desse método podem ser vistos de forma resumida na figura 5.1.

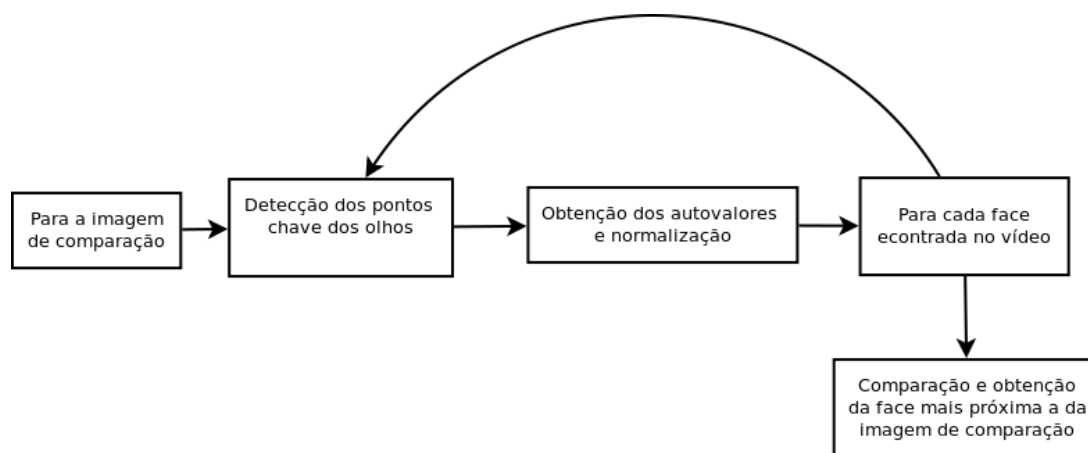


Figura 5.1: Fluxograma das etapas do método proposto.

### 5.1 Obtenção das medidas dos olhos

Inicialmente, é necessário encontrar os centros dos olhos. Para isso, utilizamos a mesma técnica da detecção de faces, apresentada no capítulo 4. Porém dessa vez a máscara e a

escala são fixas. A máscara utilizada é a "*haarcascade\_mcs\_ryghteye.xml*" e a escala é definida 1.0. Esse método também nos fornece a distância em píxel entre os centros dos olhos e as sobrancelhas. O último ponto que precisamos obter é a largura de cada olho.

Geralmente, no centro do olho, encontra-se a pupila, caracterizada por ter uma cor mais escura, em seguida o olho possui uma região branca que termina na pele ao lado do olho(mais escura que a parte branca do olho). A partir destas prerrogativas como base, tendo o centro do olho definido, percorre-se pixel a pixel, para a direita e depois para a esquerda, procurando primeiro uma região branca e, ao encontrá-la, procura-se uma região mais escura. Ao se encontrar a pele, marcamos esses dois pontos e assim obtemos a largura do olho. Repetimos isso para encontrar a dimensão de ambos os olhos e em seguida tiramos a média aritmética da largura dos olhos e da distância das sobrancelhas para os centros dos olhos.

Com isso obtemos três pontos: a distância média das sobrancelhas, a distância entre os olhos e a largura média dos olhos. Sendo chamados de A, B e C respectivamente.

## 5.2 Extração da métrica

Com esses três valores A, B e C obtidos, montamos os vetores

$$F = \begin{bmatrix} A & B & C \end{bmatrix} \text{ e } F^T = \begin{bmatrix} A \\ B \\ C \end{bmatrix} \quad (5.1)$$

Em seguida, obtemos a matriz M pela correlação cruzada do vetor F, como:

$$M = F.F^T = \begin{bmatrix} A & B & C \end{bmatrix} \times \begin{bmatrix} A \\ B \\ C \end{bmatrix} \quad (5.2)$$

Resultando na matriz:

$$M = \begin{bmatrix} A^2 & A.B & A.C \\ A.B & B^2 & B.C \\ A.C & B.C & C^2 \end{bmatrix} \quad (5.3)$$

Com a matriz M, calculamos os seus autovalores, o que resultará em um vetor:

$$v = \begin{bmatrix} X_1 & X_2 & X_3 \end{bmatrix} \quad (5.4)$$

O cálculo dos autovalores é feito utilizando a função *eigen* do OpenCV, e tem sua declaração como:

```
bool eigen(const Mat src, Mat eigenvalues, int lowindex=-1, int highindex=-1)
```

Essa função calculará os autovalores e os armazenará na matriz *eigenvalues* em ordem decrescente, por último esses valores são normalizados e colocados em valores entre 0 e 100.

## 5.3 Comparação de faces

Para cada face que foi encontrada no vídeo, é obtido o vetor normalizado e feita uma subtração entre o vetor da imagem de comparação e os vetores das faces obtidas do vídeo. A menor diferença é armazenada. Para que não seja escolhida simplesmente a menor diferença, a provável face deve ter no máximo 20% de diferença em cada autovalor normalizado em comparação com os autovalores da imagem de comparação para que ele seja considerado como provável suspeito.

Ao finalizar a comparação com todas as faces encontradas no vídeo e obter a face com a menor diferença entre os autovalores, a face do provável suspeito será exibida em outra janela.

# Capítulo 6

## Resultados Obtidos

O trabalho foi dividido em três partes:

- Desenvolver suporte a vídeo na ferramenta FI<sup>2</sup>
- Detectar as faces no vídeo e extraí-las
- Realizar o reconhecimento facial seguindo a métrica apresentada no capítulo 5

### 6.1 Detecção facial e extração

Para a detecção facial, foi inserida uma nova ferramenta, onde é escolhida a máscara que será utilizada, a escala e a suavidade espacial(para que o mesmo rosto, ao se movimentar pouco não seja extraído como um novo rosto).

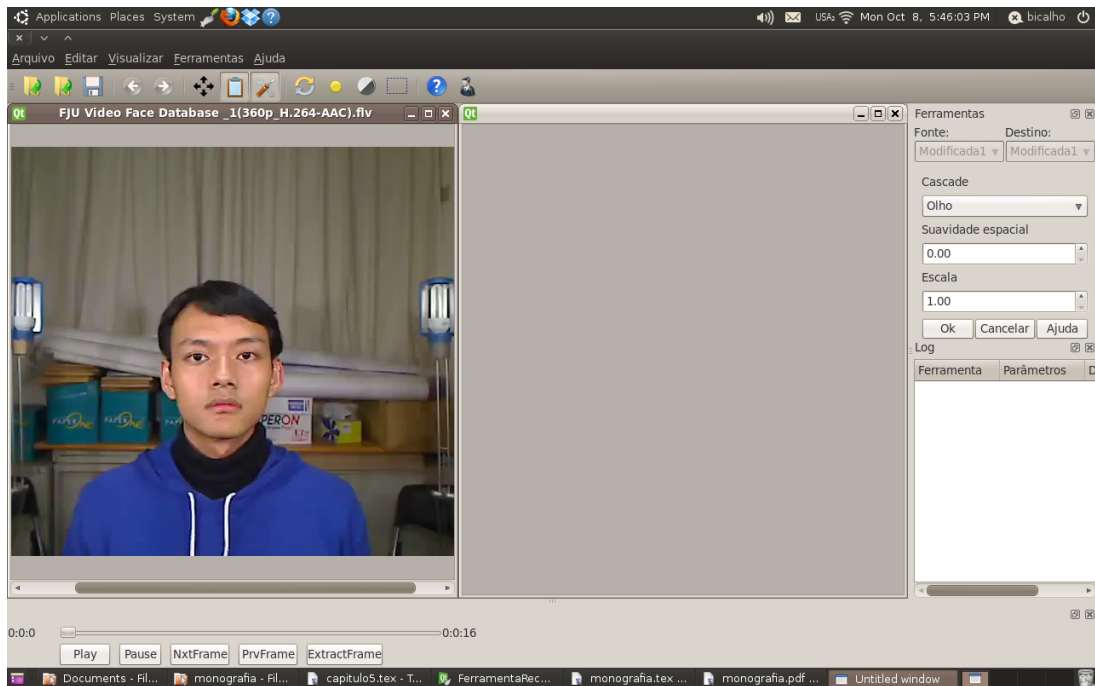


Figura 6.1: Exemplo das configurações que podem ser escolhidas na ferramenta de identificação facial.

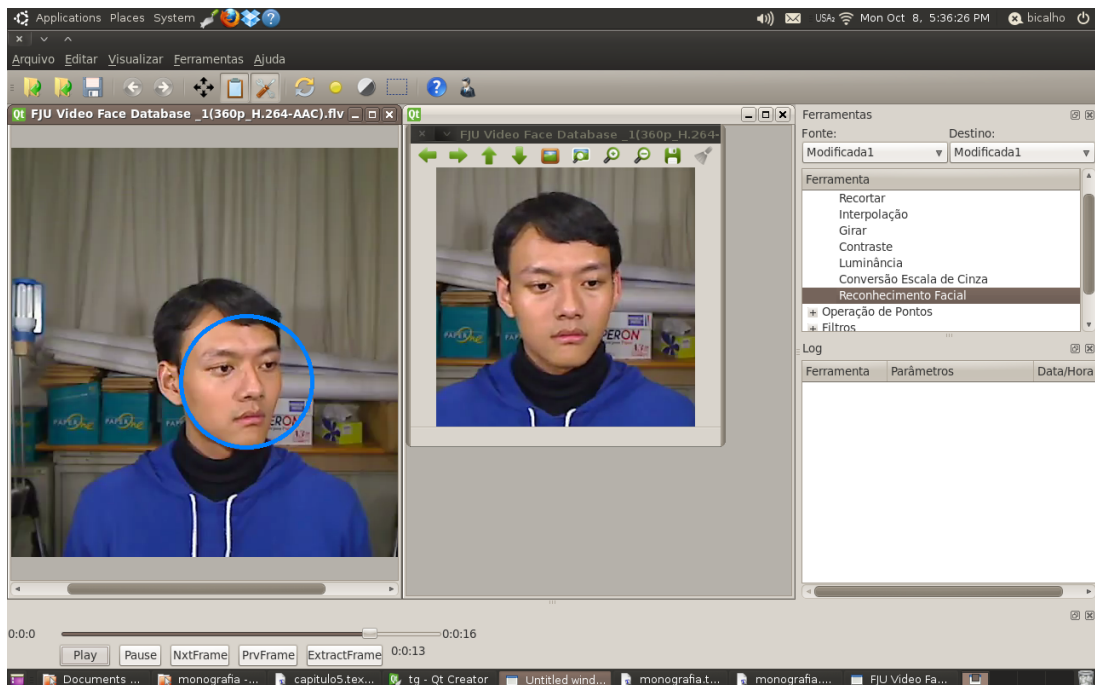


Figura 6.2: Exemplo da ferramenta em funcionamento, utilizando a máscara para rostos frontais. O rosto encontrado é extraído em uma nova janela.



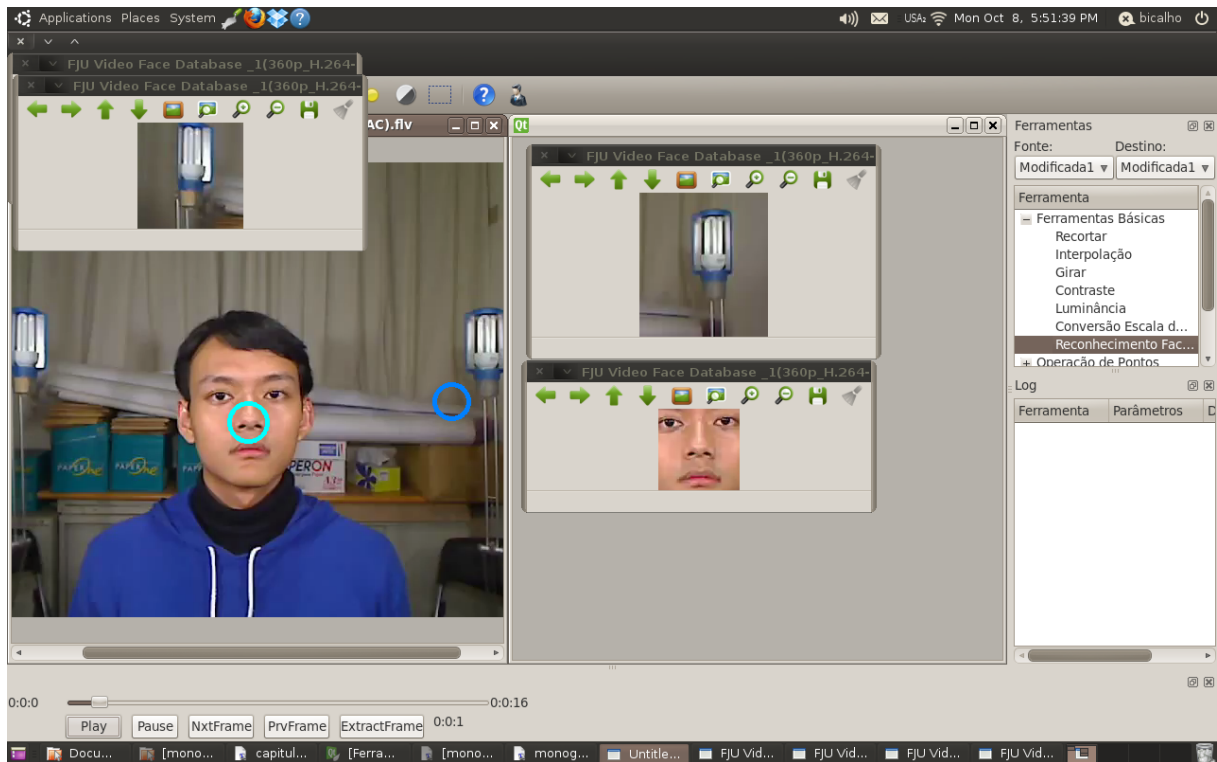


Figura 6.3: Exemplo da ferramenta em funcionamento, utilizando a máscara para narizes. Com esse exemplo é possível observar a ocorrência de falsos positivos, isto é, objetos que não são narizes sendo detectados.

## 6.2 Reconhecimento facial

O reconhecimento possui algumas restrições para o seu funcionamento. Para que seja usável, é necessário que o vídeo e a imagem de comparação preencham alguns requisitos:

- O vídeo deve ter a face de forma frontal e com os olhos fixos na câmera.
- A imagem de comparação deve conter apenas uma face, com os olhos fixos na câmera.
- As condições de luz devem ser as mesmas em ambas as imagens.



Figura 6.4: Exemplo de face utilizada para comparação.

Tendo a imagem e um vídeo que cumpram essas condições, podemos realizar o reconhecimento.

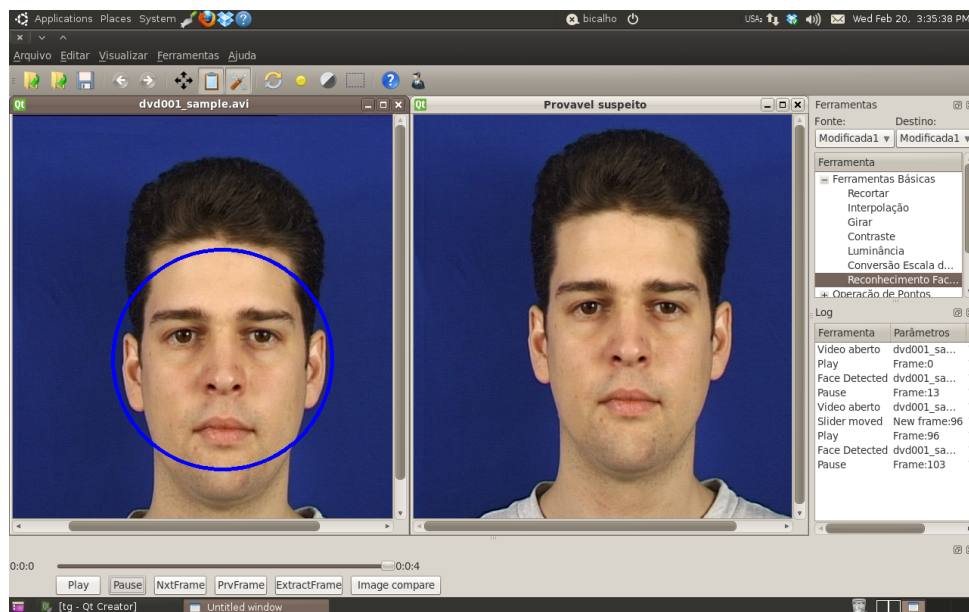


Figura 6.5: Exemplo do reconhecimento, utilizando a imagem 6.4. Apesar de na imagem de comparação os olhos estarem com formas diferentes, ainda foi possível realizar o reconhecimento devido à margem de erro.

Porém, nem sempre o reconhecimento é capaz de detectar devido a mudanças, mesmo que pequenas, na posição dos olhos.

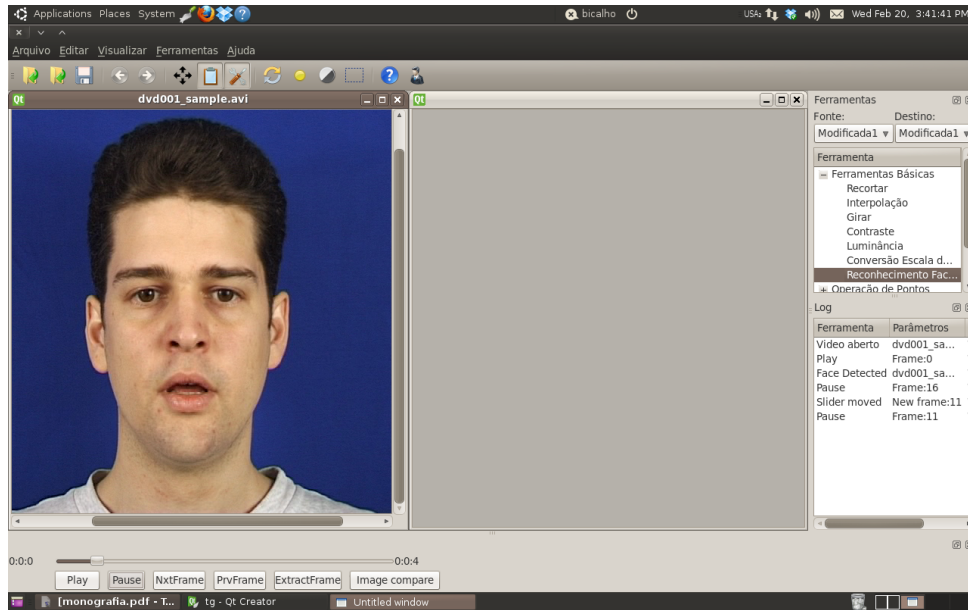


Figura 6.6: Utilizando a mesma imagem de comparação, nenhuma face foi detectada. Ao encontrar uma face compatível, ela é recortada para a *SubWindow* ao lado. O motivo de não ter detectado, é a abertura dos olhos.

### 6.2.1 Imagem de comparação 2



Figura 6.7: Exemplo de face utilizada para comparação.

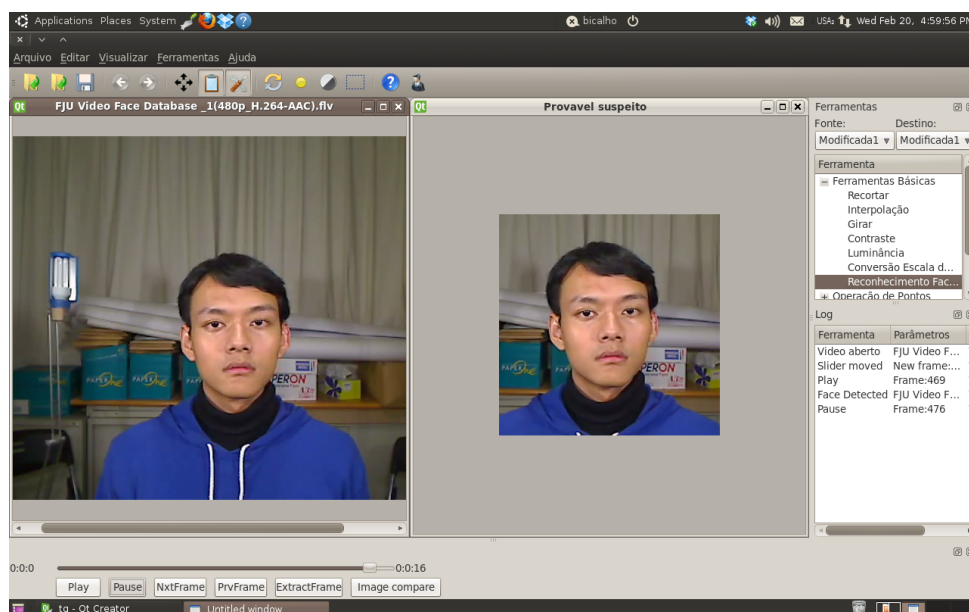


Figura 6.8: Exemplo onde mesmo com o rosto não estando completamente voltado para câmera, foi possível realizar o reconhecimento.

Os testes foram realizados utilizando a máscara "*haarcascade\_frontalface\_alt.xml*" e escala 1.8 na detecção. Dessa forma é possível que a detecção dos rostos não fique lenta e ainda eficiente, se comparado com escalas inferiores.

A margem de erro adotada para cada autovalor é de 20%, porém nem sempre o resultado obtido é razoável.

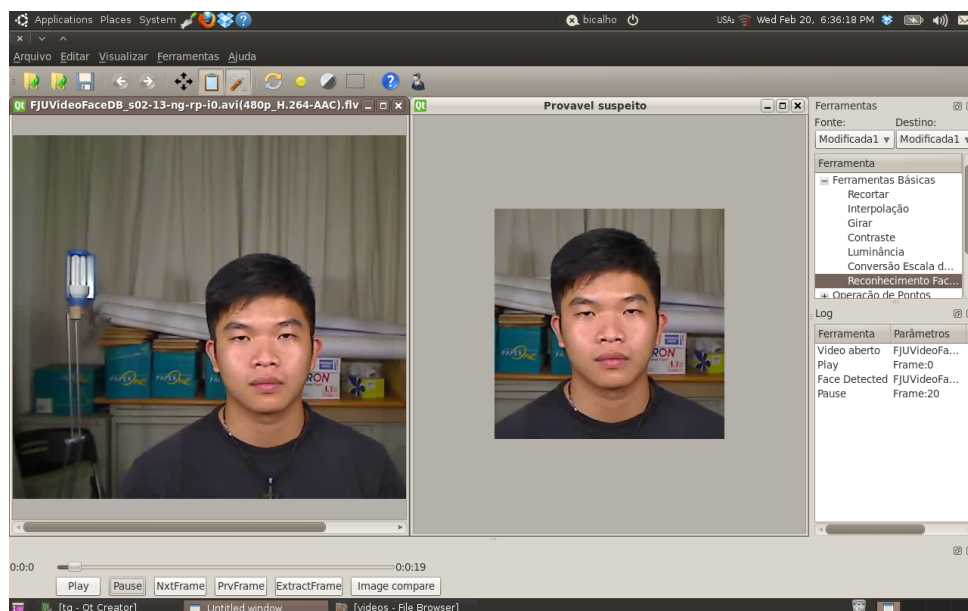


Figura 6.9: Exemplo com margem de erro de 20% utilizando a imagem de comparação acima, onde o rosto encontrado não é o mesmo indivíduo da imagem.

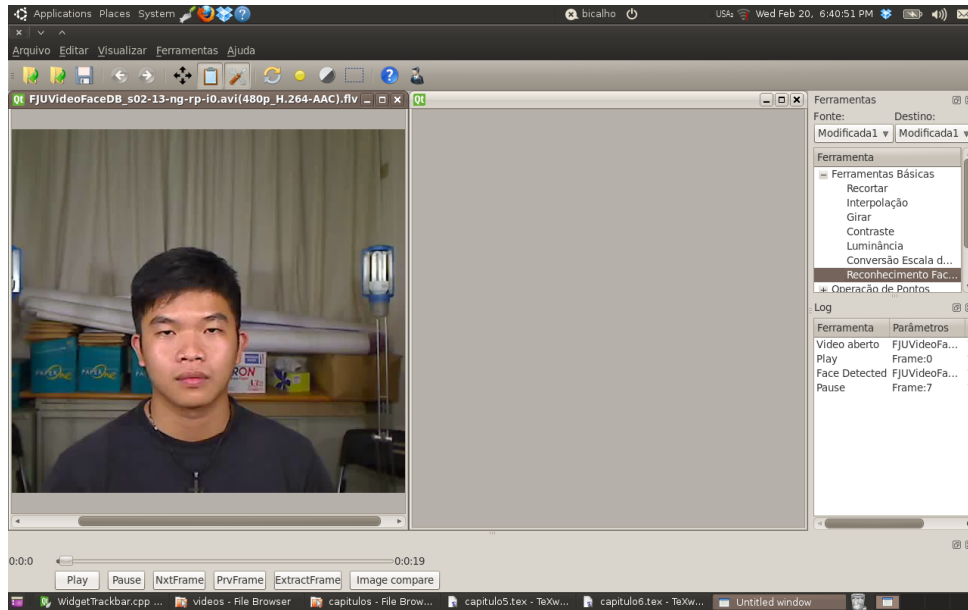


Figura 6.10: Diminuindo a margem de erro para 10%, o indivíduo não é mais reconhecido como sendo o mesmo sujeito da imagem de comparação.

Com a redução da margem de erro, é possível eliminar alguns falsos positivos, porém pode acabar fazendo com que se perca verdadeiros positivos. O ajuste depende da tolerância que se deseja adotar.

## 6.3 Avaliação da Métrica Proposta

Foram realizados testes em um conjunto de 5 vídeos, contendo 1 indivíduo diferente em cada vídeo. Os vídeos testados foram retirados da base de dados *FJU Video Face Database* e têm como características serem rostos frontais, com luminância adequada e boa qualidade. A tabela abaixo descreve os resultados:

	VP	VN	FP	FN	Precisão	Revocação
Vídeo 1	1	1	3	0	0.25	1
Vídeo 2	1	1	3	0	0.25	1
Vídeo 3	1	1	3	0	0.25	1
Vídeo 4	1	1	3	0	0.25	1
Vídeo 5	1	4	0	0	1	1
Total	5	8	12	0	0.294117647	1

Tabela 6.1: Tabela com os resultados obtidos no teste. VP = verdadeiro positivo, VN = verdadeiro negativo, FP = falso positivo, FN = falso negativo.

O *F-Measure* obtido a partir dos dados da tabela foi de 0.4545.

Como é visto na tabela 6.1, o *recall* obtido para todos os vídeos é máximo, isso significa que todos os verdadeiros positivos foram encontrados e nenhum falso negativo. Apesar disso, o *f-measure* foi relativamente baixo devido ao grande número de falsos positivos.

# Capítulo 7

## Conclusão

O reconhecimento facial vem ganhando muita importância nos dias de hoje, e a ferramenta FI<sup>2</sup>, como uma ferramenta de processamento de imagens forense, necessitava de um módulo para atender essa demanda. Para que isso fosse alcançado, foi necessário inserir suporte a vídeo no sistema, além disso é possível que todos os rostos do sistema sejam extraídos automaticamente de vídeos, facilitando assim o trabalho dos peritos. Com essas novas funcionalidades, a ferramenta se torna ainda mais útil nos casos de investigação forense.

De acordo com os objetivos propostos no capítulo 1, é possível observar que todos eles foram atingidos. O módulo de reconhecimento facial ainda precisa de aprimoramentos para que possa ser totalmente usável, como por exemplo permitir que sejam executados vários vídeos em sequência.

O método utilizado para o reconhecimento também pode passar por algumas alterações para melhorar a sua precisão, uma possível solução seria armazenar na lista de faces apenas a aparição da face com a melhor norma frontal, dessa forma, faces que estivessem de lado não seriam utilizadas na comparação.

Com a adição do suporte à vídeo e do módulo de reconhecimento facial, a gama de ferramentas que podem ser adicionadas à ferramenta aumentou significativamente. Um exemplo de ferramenta que pode ser implementada agora é o reconhecimento facial através de retrato falado.



# Referências

- [1] David A. Forsyth and Jean Ponce. *Computer Vision A Modern Approach*. Prentice Hall, New Jersey, 2003. 1
- [2] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Prentice Hall, New Jersey, 2002. 1
- [3] André P. Henriques, Tauan de O. Naves, Gustavo C. Bicalho, Flávio de B. Vidal, and Díbio L. Borges. Fi2 - uma proposta de ferramenta para investigação forense em imagens. *Conferência Internacional de Ciências Forenses em Multimídia e Segurança Eletrônica - ICMedia 2012*, 2012. 1, 12
- [4] Anil K. Jain, Brendan Klare, and Unsang Park. Face recognition: Some challenges in forensics. In *FG*, pages 726–733, 2011. v, 3, 4, 5, 6, 7, 8, 9, 10
- [5] Robert Langaière. *OpenCV 2 Computer Vision Application Programming Cookbook*. Packt, Birmingham, 2011. 2
- [6] Dan Manson, Anna Carlin, Steve Ramos, Alain Gyger, Matthew Kaufman, and Jeremy Treichelt. Is the open way a better way? digital forensics using open source tools. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, HICSS '07, pages 266b–, Washington, DC, USA, 2007. IEEE Computer Society.
- [7] Nokia. Qt reference documentation. <http://doc.qt.nokia.com/4.7-snapshot/tutorials.html>. Acessado em 22/04/2012. 2, 13
- [8] OpenCV. Opencv 2.1 c++ reference. <http://opencv.willowgarage.com/documentation/cpp/index.html>. Acessado em 22/04/2012. 2, 13
- [9] Jonathon P. Phillips, Hyeonjoon Moon, Syed A. Rizvi, and Patrick J. Rauss. The FERET Evaluation Methodology for Face-Recognition Algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10):1090–1104, 2000. 3
- [10] SmartGate. Smartgate. <http://www.customs.gov.au/smartgate/default.asp>. Acessado em 13/05/2012. 3
- [11] StarWitness. Starwitness. <http://starwitnessinfo.blogspot.com.br/>. Acessado em 16/09/2012. 12
- [12] IMIX Vision Support Systems. Impress. <http://www.imix.nl/impress/index.htm>. Acessado em 16/09/2012. 11

- [13] Ocean Systems. dtective. <http://www.oceansystems.com/dtective/>. Acessado em 16/09/2012. 11